Beschreibung

Verfahren zur verschlüsselten Datenübertragung über ein Kommunikationsnetz

Die Erfindung betrifft ein Verfahren zur verschlüsselten Datenübertragung, sowie ein entsprechendes Computerprogrammprodukt und ein Kommunikationssystem, insbesondere für die Teilnehmer eines Automatisierungssystems.

Aus dem Stand der Technik sind verschiedene Verfahren zur verschlüsselten Datenübertragung bekannt. Grundsätzlich unterscheidet man hierbei zwischen asymmetrischen und symmetrischen Verschlüsselungsverfahren.

Symmetrische Verschlüsselungsverfahren werden auch als "Private Key"-Verschlüsselung bezeichnet. Bei einer symmetrischen Verschlüsselung haben die Teilnehmer an der Kommunikation denselben geheimen Schlüssel, der sowohl für die Verschlüsselung als auch für die Entschlüsselung dient. Beispiele für aus dem Stand der Technik bekannte symmetrische Verschlüsselungsverfahren sind DES, Triple-DES, RC2, RC4, IDEA, Skipjack.

Ein gemeinsamer Nachteil von aus dem Stand der Technik bekannten symmetrischen Verschlüsselungsverfahren ist, dass vor Beginn der verschlüsselten Kommunikation die symmetrischen Schlüssel zu den einzelnen Teilnehmern übertragen werden müssen, wobei diese Übertragung ausgespäht werden kann.

Bei asymmetrischen Verschlüsselungsverfahren, die auch als "Public-Key"-Verschlüsselung bezeichnet werden, dient ein Public-Key zur Verschlüsselung. Die mit dem Public-Key eines Teilnehmers verschlüsselten Daten können nur mit dem geheimen Private-Key dieses Teilnehmers entschlüsselt werden. Bekannte asymmetrische Verschlüsselungsverfahren sind Diffie-Hellmann und RSA.

Der Erfindung liegt demgegenüber die Aufgabe zugrunde, ein verbessertes Verfahren zur verschlüsselten Datenübertragung sowie ein entsprechendes Computerprogrammprodukt und Kommunikationssystem für die verschlüsselte Datenübertragung zu schaffen.

Die der Erfindung zugrunde liegenden Aufgaben werden jeweils mit den Merkmalen der unabhängigen Patentansprüche gelöst. Bevorzugte Ausführungsformen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

Erfindungsgemäß wird für die geschützte Datenübertragung, beispielsweise über ein öffentliches Kommunikationsnetz wie das Internet, ein symmetrisches Verschlüsselungsverfahren verwendet. Im Unterschied zum Stand der Technik erfolgt dabei keine Verteilung des geheimen symmetrischen Schlüssels an die einzelnen Teilnehmer des Kommunikationsnetzes, sondern der symmetrische Schlüssel wird in den einzelnen Teilnehmern jeweils lokal erzeugt.

Hierzu werden Daten, die einem stochastischen Prozess entnommen sind, in die einzelnen Teilnehmer eingegeben. Auf dieser Grundlage werden dann in den Teilnehmern jeweils lokal identische symmetrische Schlüssel erzeugt, die im Weiteren für die verschlüsselte Datenübertragung zwischen den Teilnehmern verwendet werden.

Nach einer bevorzugten Ausführungsform der Erfindung werden die Daten, die die Grundlage für die Erzeugung der symmetrischen Schlüssel in den Teilnehmern bilden, mittels eines Zufallszahlgenerators erzeugt, der einen stochastischen Prozess, wie z. B. Widerstandsrauschen oder einen radioaktiven Zerfallsprozess für die Zufallszahlenerzeugung nutzt. Im Vergleich zu auf Generatorpolynomen basierenden Zufallszahlengeneratoren hat ein solcher Zufallszahlengenerator den Vorteil, dass es sich nicht um Pseudo-Zufallszahlen handelt. Das Generatorpolynom kann nämlich prinzipiell durch einen Angreifer

durch Auswertung der Kommunikation der Teilnehmer ermittelt werden, insbesondere wenn es sich um zyklische Kommunikation handelt.

Nach einer weiteren bevorzugten Ausführungsform wird mindestens ein Messwert aus einem stochastischen Prozess ermittelt. Beispielsweise werden die für die Erzeugung der symmetrischen Schlüssel benötigten Daten aus den niedersignifikanten Bitpositionen des bzw. der Messwerte gewonnen.

Nach einer weiteren bevorzugten Ausführungsform der Erfindung wird mindestens ein zeitlich veränderlicher Parameter eines Automatisierungssystem als stochastischer Prozess genutzt. Hierfür kommen beispielsweise verschiedene Messwerte, die von Sensoren des Automatisierungssystems geliefert werden, wie z. B. Temperatur, Drehzahl, Spannung, Strom, Durchfluss, Geschwindigkeit, Konzentration, Feuchtigkeit, ... in Frage. Die entsprechenden Messwerte sind stochastisch, können aber beispielsweise periodische Komponenten aufweisen. Zur Reduktion solcher periodischen Komponenten können beispielsweise nur die niedersignifikanten Bitpositionen der Messwerte für die Bildung der symmetrischen Schlüssel herangezogen werden.

Nach einer bevorzugten Ausführungsform der Erfindung werden von zumindest zwei der Teilnehmer unabhängig voneinander stochastische Daten erfasst. Die von einem der Teilnehmer erfassten stochastischen Daten werden an den oder die anderen Teilnehmer übertragen. Insgesamt erhält jeder der Teilnehmer auf diese Art und Weise sämtliche der stochastischen Daten. Diese werden dann miteinander kombiniert, um eine Grundlage für die jeweilige Erzeugung des symmetrischen Schlüssels zu erhalten.

Nach einer weiteren bevorzugten Ausführungsform der Erfindung erfolgt die Übertragung der Daten, die die Grundlage für die symmetrische Schlüsselerzeugung in den Teilnehmern bilden,

über ein öffentliches Netz, wie beispielsweise das Internet, oder ein Ethernet, beispielsweise ein LAN, WAN oder WLAN.

Nach einer weiteren bevorzugten Ausführungsform der Erfindung erfolgt die Schlüsselerzeugung in den Teilnehmern auf Anforderung eines Master-Teilnehmers, wobei die entsprechende Anforderung über das Kommunikationsnetz zu den Teilnehmern übertragen wird. Beispielsweise erfolgt eine entsprechende Anforderung dann, wenn die Auslastung des Kommunikationsnetzes mit Nutzdatenübertragung relativ gering ist, um die ungenutzte Bandbreite für die Übertragung von Daten als Grundlage für die Schlüsselbildung in den Teilnehmern zu nutzen. Diese Vorgehensweise ist insbesondere dann vorteilhaft, wenn die Teilnehmer über das Internet kommunizieren.

Wenn dagegen zum Beispiel ein Ethernet verwendet wird, können alle Teilnehmer den Datenverkehr auf dem Ethernet "mithören". In diesem Fall kann die Schlüsselbildung in den einzelnen Teilnehmern so angestoßen werden, dass der Master-Teilnehmer ein entsprechendes Trigger-Kommando auf das Ethernet ausgibt.

Nach einer weiteren bevorzugten Ausführungsform der Erfindung erfolgt die Übertragung der stochastischen Daten und die Schlüsselerzeugung in den Teilnehmern zu vorbestimmten Zeitpunkten oder nach vorbestimmten Zeitintervallen. In dieser Ausführungsform verfügen die Teilnehmer des Kommunikationsnetzes über eine synchrone Zeitbasis.

Nach einer weiteren bevorzugten Ausführungsform der Erfindung werden verschiedene symmetrische Verschlüsselungsverfahren von den Teilnehmern zur Schlüsselerzeugung verwendet und entsprechende unterschiedliche symmetrische Schlüssel erzeugt. Für die verschlüsselte Datenübertragung wird beispielsweise periodisch zwischen den Verschlüsselungsverfahren umgeschaltet, um die Sicherheit der verschlüsselten Datenübertragung weiter zu erhöhen.

Nach einer weiteren bevorzugten Ausführungsform der Erfindung werden die Daten für die verschiedenen Verschlüsselungsverfahren durch unterschiedliche Kombinationen der von den einzelnen Teilnehmern gelieferten stochastischen Daten gebildet.

Von besonderem Vorteil ist die vorliegende Erfindung zur Anwendung bei Automatisierungssystemen. Beispielsweise können die Algorithmen zur Schlüsselbildung in den einzelnen Teilnehmern bei der Projektierung der Anlage festgelegt werden. Die entsprechenden Algorithmen zur Schlüsselbildung werden von dem Hersteller der Anlage geheim gehalten. Neben dem Schutz der verschlüsselten Datenübertragung ist damit auch ein Schutz gegen die Benutzung nicht autorisierter Komponenten, beispielsweise von einem Dritthersteller, in dem Automatisierungssystem gegeben.

Vorzugsweise werden die Algorithmen in geschützten Speicherbereichen der Automatisierungsgeräte des Automatisierungssystems gespeichert, z.B. in EPROMs oder Chipkarten, die von authorisierten Nutzern in Kartenleser der Automatisierungsgeräte eingeführt werden.

Besonders vorteilhaft ist die Anwendung der vorliegenden Erfindung für über öffentliche Netze miteinander verknüpfte Komponenten automatisierungstechnischer Anlagen. Durch die erfindungsgemäße verschlüsselte Datenübertragung zwischen den Teilnehmern einer solchen automatisierungstechnischen Anlage werden unbefugte Eingriffe Dritter vermieden, insbesondere auch dann, wenn eine drahtlose Übertragungstechnik zwischen den Teilnehmern verwendet wird.

Nach einer weiteren bevorzugten Ausführungsform der Erfindung wird die verschlüsselte Datenübertragung für die Zwecke der Fernwartung oder des so genannten Teleservice der Anlage verwendet. Auch hier bietet das erfindungsgemäße Datenübertragungsverfahren einen Schutz gegen Ausspähung der übertragenen Anlagendaten bzw. manipulierende Eingriffe.

Neben einer automatisierungstechnischen Anlage kann die Erfindung vorteilhaft auch für die Zwecke der Telekommunikation zwischen Teilnehmern oder für die Zwecke der Kommunikation zwischen den Komponenten einer Kraftfahrzeug-, Schiffs-, Flugzeug- oder Eisenbahnelektronik verwendet werden.

Im Weiteren werden bevorzugte Ausführungsformen der Erfindung mit Bezugnahme auf die Zeichnungen näher erläutert. Es zeigen:

Figur 1 ein Blockdiagramm einer ersten Ausführungsform eines erfindungsgemäßen Kommunikationssystems,

Figur 2 ein Flussdiagramm einer ersten Ausführungsform des erfindungsgemäßen Datenübertragungsverfahrens,

Figur 3 die Erzeugung von Daten als Grundlage für die Schlüsselerzeugung aus einem Messwert,

Figur 4 ein Blockdiagramm einer weiteren bevorzugten Ausführungsform eines erfindungsgemäßen Kommunikationssystems,

Figur 5 ein Blockdiagramm einer bevorzugten Ausführungsform eines erfindungsgemäßen Automatisierungssystems.

Figur 1 zeigt ein Kommunikationssystem 100, in dem zumindest Teilnehmer 102 und 104 über ein Netzwerk 106 Daten austauschen können. In einer praktischen Ausführungsform kann das Kommunikationssystem 100 eine Vielzahl von solchen Teilnehmern beinhalten.

Die Teilnehmer 102, 104 des Kommunikationssystems 100 haben jeweils ein Programm 108 für ein symmetrisches Verschlüsselungsverfahren. Mit Hilfe der Programme 108 können auf der

Grundlage von Eingabedaten symmetrische Schlüssel gebildet werden, sowie zu übertragende Nutzdaten verschlüsselt und entschlüsselt werden.

Die Teilnehmer 102, 104 haben ferner jeweils einen Speicher 110 zur Speicherung des durch das jeweilige Programm 108 generierten symmetrischen Schlüssels.

Der Teilnehmer 102 ist mit einem Erfassungsmodul 112 verbunden; das Erfassungsmodul 112 dient zur Erfassung von stochastischen Daten aus einem stochastischen Prozess 114. Bei dem stochastischen Prozess 114 kann es sich beispielsweise um das Spannungssignal eines rauschenden Widerstandes handeln.

Ferner ist der Teilnehmer 102 mit einer Datenquelle 116 verbunden. Von der Datenquelle 116 gelieferte Daten sollen von dem Teilnehmer 102 über das Netzwerk 106 zu dem Teilnehmer 104 übertragen werden.

Beim Betrieb des Kommunikationssystems 100 werden von dem Erfassungsmodul 112 stochastische Daten aus dem stochastischen Prozess 114 erfasst. Die stochastischen Daten werden in den Teilnehmer 102 eingegeben. Die stochastischen Daten werden von dem Teilnehmer 102 über das Netzwerk 106 an den Teilnehmer 104 übertragen. Dies kann verschlüsselt oder unverschlüsselt erfolgen.

In dem Teilnehmer 102 wird das Programm 108 gestartet, um auf der Grundlage der von dem Erfassungsmodul 112 gelieferten stochastischen Daten einen symmetrischen Schlüssel zu erzeugen, der in dem Speicher 110 gespeichert wird. Entsprechend wird das Programm 108 in dem Teilnehmer 104 gestartet, um die von dem Teilnehmer 102 über das Netzwerk 106 empfangenen stochastischen Daten zur Erzeugung desselben symmetrischen Schlüssels zu verwenden, der in dem Speicher 110 des Teilnehmers 104 gespeichert wird.

Wenn weitere Teilnehmer in dem Kommunikationssystem 100 vorhanden sind, erhalten auch die weiteren Teilnehmer die stochastischen Daten von dem Teilnehmer 102 über das Netzwerk 106 und erzeugen jeweils lokal den symmetrischen Schlüssel mit Hilfe des jeweiligen Programms 108.

Daten, die von der Datenquelle 116 an den Teilnehmer 102 geliefert werden, können nun verschlüsselt über das Netzwerk 106 zu dem Teilnehmer 104 übertragen werden. Hierzu werden die zu übertragenden Nutzdaten mit Hilfe des Programms 108 des Teilnehmers 102 und des in dem Speicher 110 des Teilnehmers 102 gespeicherten symmetrischen Schlüssels verschlüsselt.

Die verschlüsselten Nutzdaten werden über das Netzwerk 106 übertragen und von dem Teilnehmer 104 empfangen. Dort werden die Daten von dem Programm 108 des Teilnehmers 104 mit Hilfe des in dem Speicher 110 des Teilnehmers 104 gespeicherten symmetrischen Schlüssels entschlüsselt.

Die Erzeugung der stochastischen Daten als Grundlage für die Erzeugung der symmetrischen Schlüssel in den Teilnehmern 102, 104 kann dabei durch einen stochastischen Zufallszahlengenerator erfolgen, der z. B. die Ausgangsspannung eines rauschenden Widerstandes als stochastischen Prozess verwendet.

Alternativ können auch die von der Datenquelle 116 gelieferten Daten als stochastische Daten als Grundlage für die Erzeugung der symmetrischen Schlüssel verwendet werden. Dies ist insbesondere dann vorteilhaft, wenn die Datenquelle 116 Messwerte von zeitlich veränderlichen Größen oder Parametern, beispielsweise eines Automatisierungssystems, liefert. Beispielsweise sind bestimmte Prozessparameter in einem solchen Automatisierungssystem wie die Temperatur, Druck, Drehzahl, etc. nicht deterministisch, sondern mehr oder weniger zufällig mit mehr oder weniger periodischen Komponenten. Ein entsprechender von der Datenquelle 116 gelieferter Messwert

kann also als stochastisches Datum für die symmetrische Schlüsselerzeugung verwendet werden, wobei sich in diesem Fall ein separates Erfassungsmodul 112 bzw. ein zusätzlicher stochastischer Prozess 114 erübrigen.

Die Figur 2 zeigt ein entsprechendes Flussdiagramm. In dem Schritt 200 werden stochastische Daten erfasst. Hierbei kann es sich um von einen Zufallsgenerator gelieferte stochastische Daten handeln oder um die Nutzdaten, die von einer Datenquelle geliefert werden. In dem Schritt 202 werden die stochastischen Daten an die Teilnehmer des Kommunikationssystems übertragen. Dies kann verschlüsselt oder unverschlüsselt über ein öffentliches Netzwerk erfolgen.

In dem Schritt 204 werden durch die Teilnehmer auf der Basis der stochastischen Daten jeweils identische symmetrische Schlüssel lokal erzeugt. Hierzu dient ein geheimes Verschlüsselungsverfahren, welches in den Teilnehmern jeweils durch ein Computerprogramm implementiert ist.

Jeder der Teilnehmer, der die stochastischen Daten in dem Schritt 202 empfangen hat, gibt also diese stochastischen Daten in das Computerprogramm ein, um einen symmetrischen Schlüssel zu erzeugen, der von dem jeweiligen Teilnehmer lokal abgespeichert wird.

Im Ergebnis verfügen also alle Teilnehmer über den symmetrischen Schlüssel, ohne dass dieser über das Netzwerk 106 übertragen worden ist. Auch durch Ausspähung der Übertragung der stochastischen Daten über das Netzwerk 106 kann ein Dritter nicht in den Besitz des Schlüssels kommen, da hierfür das geheime Verschlüsselungsverfahren, bzw. das entsprechende Computerprogramm erforderlich ist. Um unauthorisierte Zugriffe auf das Computerprogramm zu vermeiden, ist dies vorzugsweise in einem geschützten Speicherbereich, beispielsweise in einem EPROM oder auf einer Chipkarte gespeichert.

Nachdem die identischen symmetrischen Schlüssel basierend auf den stochastischen Daten in den einzelnen Teilnehmern erzeugt worden sind, werden diese Schlüssel für die geschützte Kommunikation zwischen den Teilnehmern in dem Schritt 206 verwendet.

Die Figur 3 zeigt ein Ausführungsbeispiel für die Erzeugung stochastischer Daten als Grundlage für die Generierung der symmetrischen Schlüssel. Beispielsweise wird von der Datenquelle 116 (vergleiche Figur 1) ein Messwert 300 geliefert, der beispielsweise eine Länge von 32 Bit hat. Beispielsweise werden nur die acht niederwertigsten Bitpositionen ("Least significant bits" - LSB) des Messwertes 300 für die Schlüsselgenerierung verwendet.

Mit anderen Worten bilden also die niederwertigsten Bitpositionen des Messwertes 300 die stochastischen Daten, welche für die Schlüsselerzeugung verwendet werden. Die Verwendung nur der niederwertigsten Bitpositionen des Messwertes 300 hat dabei gegenüber der Verwendung des vollständigen Messwertes 300 oder nur der höchstwertigen Bitpositionen ("Most significant bits" - MSB) den Vorteil, dass periodische Anteile des Messsignals reduziert oder eliminiert werden.

Die Figur 4 zeigt ein Blockdiagramm eines Kommunikationssystems 400. Elemente der Figur 4, die Elementen der Ausführungsform der Figur 1 entsprechen, sind mit um 300 erhöhten Bezugszeichen gekennzeichnet.

Bei der Ausführungsform der Figur 4 ist der Teilnehmer 402 mit den Datenquellen 418 und 420 verbunden, die fortlaufend die Messwerte a und b liefern. Der Teilnehmer 404 ist mit der Datenquelle 422 verbunden, die fortlaufend den Messwert c liefert. Bei dem Messwert a handelt es sich z. B. eine Temperatur, bei dem Messwert b um eine Drehzahl und bei dem Messwert c um einen Druck.

Die Teilnehmer 402 und 404 haben jeweils einen Speicher 424 zur Speicherung der Messwerte a, b und c. Ferner haben die Teilnehmer 402 und 404 jeweils einen Speicher 426 zur Speicherung der symmetrischen Schlüssel S1 und S2. Der Schlüssel S1 wird von dem Programm 408 auf der Grundlage einer Kombination der Messwerte a und c und der Schlüssel S2 auf der Grundlage der Messwerte a und b erzeugt.

Beim Betrieb des Kommunikationssystems 400 werden die symmetrischen Schlüssel S1 und S2 in den Teilnehmern 402 und 404 sowie in weiteren grundsätzlich gleich aufgebauten Teilnehmern erzeugt.

Hierzu werden die zu einem bestimmten Zeitpunkt von den Datenquellen 418, 420, 422 abgegebenen Messwerte a, b bzw. c in den Speicher 424 gespeichert. Das heißt, der Teilnehmer 402 speichert in seinem Speicher 424 die Messwerte a und b und überträgt diese über das Netzwerk 406 zu den weiteren Teilnehmern, d. h. insbesondere zu Teilnehmer 404, wo die Messwerte a und b ebenfalls in dem Speicher 424 gespeichert werden.

Andererseits speichert Teilnehmer 404 den Messwert c in seinem Speicher 424 und überträgt den Messwert c über das Netzwerk 406 an die anderen Teilnehmer, d. h. insbesondere an Teilnehmer 402, wo der Messwert c ebenfalls in dem jeweiligen Speicher 424 gespeichert wird. Wie mit Bezugnahme auf die Figur 3 erläutert, werden vorzugsweise anstelle der vollständigen Messwerte nur die niederwertigsten Bitpositionen in den Speichern 424 gespeichert.

Das Programm 408 des Teilnehmers 402 kombiniert die Messwerte a und b, die in dem Speicher 424 gespeichert sind, bzw. die niederwertigsten Bitpositionen dieser Messwerte, miteinander, indem die entsprechenden Bits beispielsweise aneinander gehängt werden. Das hieraus resultierende Datenwort wird

von dem Programm 408 dazu verwendet, den Schlüssel S2 zu erzeugen.

Entsprechend wird auf der Grundlage der Messwerte a und c mit Hilfe des Programms 408 der Schlüssel S1 erzeugt. Die Schlüssel S1 und S2 werden in dem Speicher 426 des Teilnehmers 402 gespeichert. Der prinzipiell gleiche Vorgang läuft in dem Teilnehmer 404 sowie den weiteren Teilnehmern des Kommunikationssystems 400 ab, sodass in sämtlichen Teilnehmern die Schlüssel S1 und S2 vorhanden sind.

Im Weiteren erfolgt eine verschlüsselte Übertragung der Messwerte a, b und c über das Netzwerk 406, wobei zu bestimmten Zeitpunkten der Schlüssel S1 und zu bestimmten Zeitpunkten der Schlüssel S2 für die verschlüsselte Datenübertragung benutzt wird. Diese Zeitpunkte können vordefiniert oder ereignisgesteuert sein. Beispielsweise kann einer der Teilnehmer die Funktion eines Master-Teilnehmers für die Initiierung der Schlüsselerzeugung oder die Umschaltung zwischen den Schlüsseln in den verschiedenen Teilnehmern haben.

Bei dem hier betrachteten Ausführungsbeispiel werden also aus den Messwerten a, b und c durch eine vorgegebene Kombinatorik verschiedene Datenworte gebildet, die ihrerseits die Grundlage zur Erzeugung verschiedener symmetrischer Schlüssel sind. Diese Kombinatorik kann zeitlich unveränderlich sein oder zeitlich veränderlich.

Die Figur 5 zeigt ein Automatisierungssystem 500 mit den Automatisierungsgeräten 502, 504, 506, 508, 510 und 512. Die Automatisierungsgeräte 502 bis 512 sind mit einem Datenbus 514 untereinander verbunden. Hierbei kann es sich z. B. um ein Ethernet handeln. Ein weiteres Automatisierungsgerät 516 kann über ein öffentliches Netzwerk 518 wie z. B. das Internet oder eine drahtlose Mobilfunkverbindung Daten austauschen.

Jedes der Automatisierungsgeräte 502 bis 512 und 516 hat ein Verschlüsselungsprogramm 520 und ein Verschlüsselungsprogramm 522. Darüber hinaus können weitere Verschlüsselungsprogramme vorhanden sein. Die Verschlüsselungsprogramme 520 und 522 stellen jeweils unterschiedliche symmetrische Verschlüsselungsverfahren zur Verfügung.

Ferner haben die Automatisierungsgeräte 502 bis 512 und 516 jeweils einen Timer 524. Die Timer 524 sind miteinander synchronisiert, sodass eine für das Automatisierungssystem 500 einheitliche synchrone Zeitbasis geschaffen wird.

Jedes der Automatisierungsgeräte 502 bis 512 hat ferner einen Speicher 526 und einen Speicher 528. Der Speicher des Automatisierungsgerätes 502 dient zur Speicherung des "Wert 1", der von einem entsprechenden Messwertgeber 1 ausgegeben wird. Der Speicher 528 des Automatisierungsgerätes 502 dient zur Speicherung des "Wert 5", der von einem Messwertgeber 5 ausgegeben wird. Entsprechend verhält es sich für die Speicher 526 und 528 der weiteren Automatisierungsgeräte 504 bis 512, die jeweils bestimmten Messwertgebern zugeordnet sind, wie aus der Figur 5 ersichtlich. Die Messwertgeber sind in der Fig. 5 der Übersichtlichkeit halber nicht dargestellt.

Das Datenwort, welches als Grundlage zur Erzeugung eines symmetrischen Schlüssels dient, wird durch eine vorgegebene Kombinatorik erzeugt, beispielsweise aus der Verkettung der Werte 1, 2, 3 und 4. Das durch diese Verkettung erhaltene Datenwort wird jeweils in die Verschlüsselungsprogramme 520 und 522 eingegeben, um entsprechende symmetrische Schlüssel zu erzeugen.

Für die verschlüsselte Datenübertragung zwischen den Automatisierungsgeräten 502 bis 512 und 516 werden die Verschlüsselungsprogramme 520 und 522 in einer vorprojektierten zeitlichen Reihenfolge verwendet, d. h. für jeden Zeitpunkt

ist vorprojektiert, ob das Verschlüsselungsprogramm 520 oder 522 für die verschlüsselte Datenübertragung zu verwenden ist.

Bei dem Automatisierungsgerät 516 handelt es sich beispielsweise um ein Fernwartungsgerät. Auch das Automatisierungsgerät 516 erhält die Messwerte 1, 2, 3 und 4 über das Netzwerk 518, um mit Hilfe der Verschlüsselungsprogramme 520 und 522 die jeweiligen Schlüssel zu bilden. Die Übertragung der Messwerte von den Automatisierungsgeräten 502, 504 und 510 erfolgt dabei über den Datenbus 514 und das Netzwerk 518 zu dem Automatisierungsgerät 516. Nachdem die Schlüsselbildung erfolgt ist, kann von dem Automatisierungsgerät 516 eine Fernwartung durchgeführt werden, wobei die hierbei über das Netzwerk 518 übertragenen Daten gegen Ausspähung und Manipulation geschützt sind.

Das Netzwerk hat die Netzzugänge 530 und 532, über die der Datenverkehr zwischen dem Datenbus 514 und dem Automatisierungsgerät 516 erfolgt. Bei der Übertragung über das Netzwerk 518 kann eine weitere Verschlüsselung vorgenommen werden, indem die bereits verschlüsselten Daten nochmals verschlüsselt werden. Hierdurch wird die Sicherheit gegen Angriffe von außen weiter erhöht.

Dies ist insbesondere vorteilhaft, wenn es sich bei dem Netzwerk 518 um ein öffentliches Netz handelt. Die weitere Verschlüsselung für die Übertragung über das Netzwerk 518 kann analog zu der Figur 1 erfolgen, wobei der Netzzugang 530 die Rolle des Teilnehmer 102 und der Netzzugang 532 die Rolle des Teilnehmers 104 einnimmt.

Von besonderem Vorteil ist, dass die geschützte Datenübertragung zwischen den Automatisierungsgeräten unabhängig von allgemeinen Sicherheitsinfrastrukturen, wie z. B. von zentralen Trustzentren, erfolgt, sondern auf zeitlich veränderlichen Daten, die aus der Anlage selber herrühren, beruht. Von weiterem Vorteil ist, dass aufgrund der geheimen Verschlüsse-

lungsprogramme 520, 522 auch eine implizite Authentifizierung der Automatisierungsgeräte erfolgt. Nicht autorisierte Automatisierungsgeräte, für die die Anlage nicht zugelassen ist, oder Automatisierungsgeräte von Fremdherstellern, die nicht über die erforderlichen Lizenzen verfügen, haben nicht die geheimen Verschlüsselungsprogramme 520, 522 und können daher auch nicht in dem Automatisierungssystem eingesetzt werden.

Zur weiteren Erhöhung der Sicherheit kann in den einzelnen Automatisierungsgeräten jeweils eine Liste von Verschlüsselungsprogrammen geladen werden. Vorzugsweise erfolgt das Laden dieser Verschlüsselungsprogramme im Offlinebetrieb des Automatisierungssystems, um ein Ausspähen der Verschlüsselungsprogramme zu vermeiden. Beispielsweise werden die Verschlüsselungsprogramme in geschützten Speicherbereichen von EPROMs oder Chipkarten gespeichert.

Die Wechselzeitpunkte für den Wechsel der Verschlüsselungsprogramme und der dazugehörigen Schlüssel können kommandogesteuert von einem der Automatisierungsgeräte bestimmt werden, welches damit die Funktion eines Masters einnimmt. Alternativ können die Wechselzeitpunkte durch vorgegebene absolute Zeitpunkte projektiert sein oder zyklisch bzw. periodisch erfolgen.

Alternativ kann auch ein von Zufallswerten der Anlage gespeister Algorithmus für die Festlegung der Wechselzeitpunkte verwendet werden. Eine weitere Möglichkeit ist, dass eine Auslastung des Datenbusses 514 überwacht wird und die Schlüsselerzeugung bzw. der Wechsel der Verschlüsselungsprogramme zu einem Zeitpunkt initiiert wird, zu dem die Auslastung des Datenbusses 514 gering ist. Dies hat den Vorteil, dass ungenutzte Bandbreite des Datenbusses 514 für die Übertragung der Messwerte zu den einzelnen Automatisierungsgeräten verwendet werden kann.

Patentansprüche

1. Verfahren zur Datenübertragung mit folgenden Schritten:

- Eingabe von ersten Daten aus einem stochastischen Prozess (114) in zumindest erste und zweite Teilnehmer (102, 104; 402, 404; 502, 504, 506, 508, 510, 512, 516) eines Kommunikationsnetzes (100, 106; 400, 406; 500, 514, 518),

- in jedem der zumindest ersten und zweiten Teilnehmer: Erzeugung eines symmetrischen Schlüssels (S1, S2), basierend auf den ersten Daten und Speicherung des symmetrischen Schlüssels für eine verschlüsselte Datenübertragung zwischen den zumindest ersten und zweiten Teilnehmern.

2. Verfahren nach Anspruch 1, wobei die ersten Daten über das Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) übertragen werden.

3. Verfahren nach Anspruch 1 oder 2, wobei die ersten Daten durch Erfassung von mindestens einem Messwert aus dem stochastischen Prozess (114) gewonnen werden.

4. Verfahren nach Anspruch 1, 2 oder 3, wobei es sich bei dem stochastischen Prozess um einen zeitlich veränderlichen Parameter eines Automatisierungssystems (500) handelt.

5. Verfahren nach einem der vorhergehenden Ansprüche 1 bis 4, wobei die ersten Daten aus niedersignifikanten Bit-Positionen (LSB) eines oder mehrerer Messwerte gewonnen werden.

6. Verfahren nach einem der vorhergehenden Ansprüche 1 bis 5, wobei jeder der zumindest ersten und zweiten Teilnehmer stochastische Daten erfasst, aus denen die ersten Daten gebildet werden.

7. Verfahren nach Anspruch 6, wobei die ersten Daten aus den stochastischen Daten durch eine vorgegebene Kombinatorik gebildet werden.

8. Verfahren nach Anspruch 6 oder 7, wobei die stochastischen Daten über das Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) übertragen werden.

9. Verfahren nach einem der vorhergehenden Ansprüche 1 bis 8, wobei die Erzeugung des symmetrischen Schlüssels in den Teilnehmern auf Anforderung eines Master-Teilnehmers des Kommunikationsnetzes erfolgt.

10. Verfahren nach einem der vorhergehenden Ansprüche 1 bis 9, wobei die Erzeugung des symmetrischen Schlüssels zu vorbestimmten Zeitpunkten oder nach vorbestimmten Zeitintervallen in den zumindest ersten und zweiten Teilnehmern erfolgt.

11. Verfahren nach einem der vorhergehenden Ansprüche 1 bis 10, wobei die Übertragung der ersten Daten oder der stochastischen Daten zu einem Zeitpunkt geringer Auslastung des Kommunikationsnetzes erfolgt.

12. Verfahren nach einem der vorhergehenden Ansprüche 1 bis 11, wobei die Übertragung der ersten Daten oder der stochastischen Daten mit einem asymmetrischen Verschlüsselungsverfahren erfolgt.

13. Verfahren nach einem der vorhergehenden Ansprüche 1 bis 12, wobei jeder der zumindest ersten und zweiten Teilnehmer über Mittel (108; 408) für erste und zweite Verschlüsselungsverfahren verfügt, wobei basierend auf den ersten Daten jeweils erste und zweite symmetrische Schlüssel erzeugt werden, und für die verschlüsselte Datenübertragung in zeitlicher Reihenfolge zwischen den ersten und zweiten Verschlüsselungsverfahren gewechselt wird.

14. Verfahren nach Anspruch 13, wobei zur Erzeugung der ersten und zweiten Schlüssel in jedem der zumindest ersten und zweiten Teilnehmer verschiedene erste Daten durch unterschiedliche Kombinatorik der stochastischen Daten gebildet werden.

15. Computerprogrammprodukt, insbesondere digitales Speichermedium, mit Programmmitteln zur Durchführung der folgenden Schritte:

- Eingabe von ersten Daten aus einem stochastischen Prozess (114) in zumindest erste und zweite Teilnehmer (102, 104; 402, 404; 502, 504, 506, 508, 510, 512, 516) eines Kommunikationsnetzes (100, 106; 400, 406; 500, 514, 518),

- in jedem der zumindest ersten und zweiten Teilnehmer: Erzeugung eines symmetrischen Schlüssels (S1, S2), basierend auf den ersten Daten und Speicherung des symmetrischen Schlüssels für eine verschlüsselte Datenübertragung zwischen den zumindest ersten und zweiten Teilnehmern.

16. Computerprogrammprodukt nach Anspruch 15, wobei die ersten Daten durch Erfassung eines Messwerts aus dem stochastischen Prozess (114) gewonnen werden.

17. Computerprogrammprodukt nach Anspruch 15 oder 16, wobei die ersten Daten aus niedersignifikanten Bit-Positionen (LSB) eines oder mehrerer Messwerte gewonnen werden.

18. Kommunikationssystem mit zumindest ersten und zweiten Teilnehmern (102, 104; 402, 404; 502, 504, 506, 508, 510, 512, 516) und einem Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) für eine Datenübertragung zwischen den zumindest ersten und zweiten Teilnehmern, und mit:

- Mitteln (112) zur Eingabe von ersten Daten aus einem stochastischen Prozess (114) in die zumindest ersten und zweiten Teilnehmer,

- in jedem der zumindest ersten und zweiten Teilnehmer: Mittel (108; 408) zur Erzeugung eines symmetrischen Schlüssels basierend auf den ersten Daten und Mittel (110; 426; 520, 522) zur Speicherung des symmetrischen Schlüssels für eine verschlüsselte Datenübertragung zwischen den zumindest ersten und zweiten Teilnehmern.

19. Kommunikationssystem nach Patentanspruch 18, wobei es sich bei dem Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) um ein öffentliches Netz handelt.

20. Kommunikationssystem nach Patentanspruch 18 oder 19, wobei es sich bei dem Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) um das Internet handelt und ein Teilnehmer als Master-Teilnehmer ausgebildet ist, um eine Schlüsselerzeugung in den anderen Teilnehmern durch Übertragung einer entsprechenden Anforderung über das Internet auszulösen.

21. Kommunikationssystem nach Anspruch 18 oder 19, wobei es sich bei dem Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) um ein Ethernet handelt.

22. Kommunikationssystem nach Anspruch 21, wobei einer der Teilnehmer als Master-Teilnehmer ausgebildet ist, um auf das Ethernet ein Kommando zur Auslösung der Schlüsselerzeugung in den Teilnehmern auszugeben.

23. Kommunikationssystem nach einem der vorhergehenden Ansprüche 18 bis 22, wobei es sich bei den zumindest ersten und zweiten Teilnehmern um Komponenten eines Automatisierungssystems (500) handelt.

24. Kommunikationssystem nach einem der vorhergehenden Ansprüche 18 bis 23, wobei zumindest einer der Teilnehmer (516) zur Durchführung einer Fernwartung ausgebildet ist.

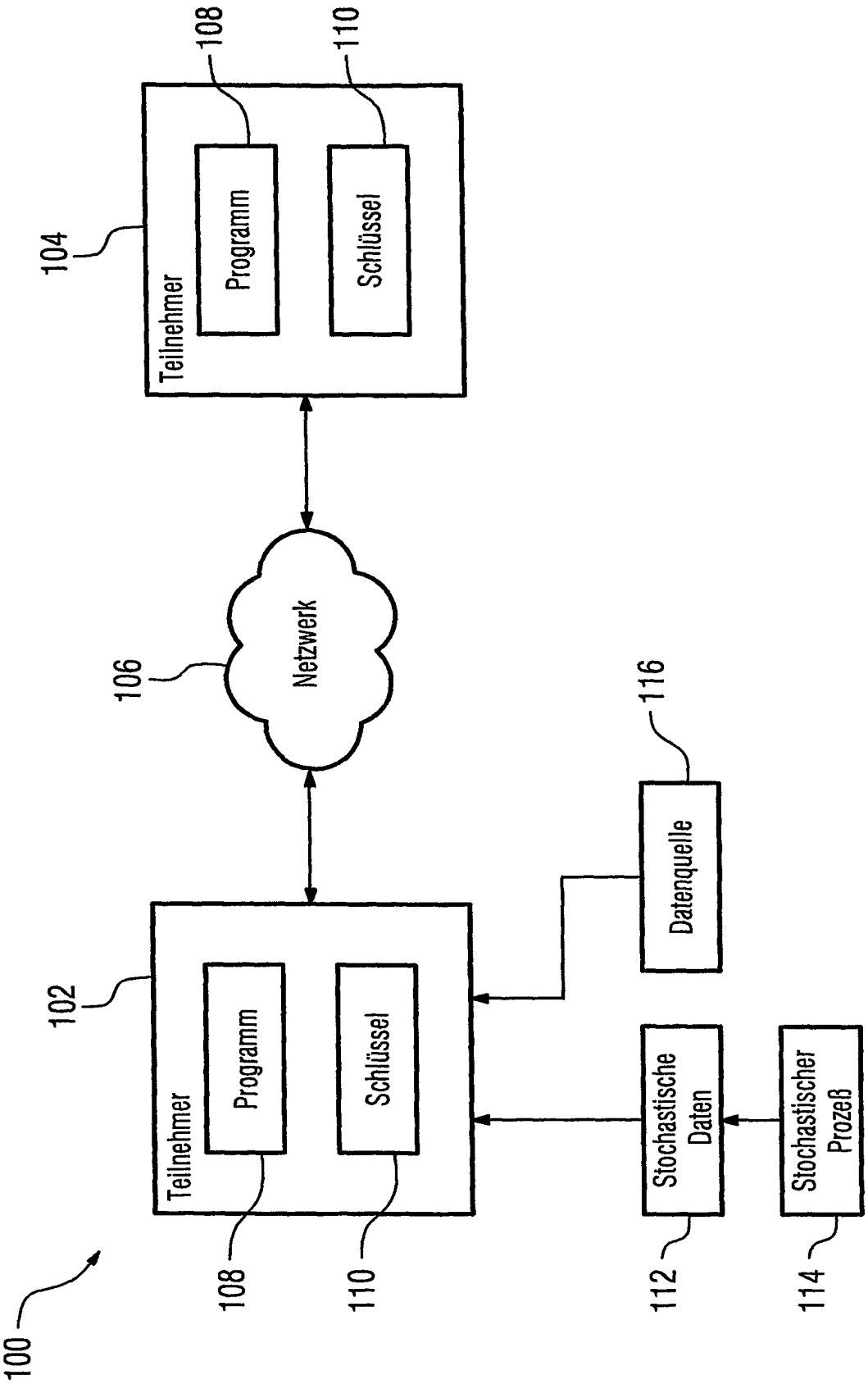

100
102
Teilnehmer
Programm
Schlüssel
104
Teilnehmer
Programm
Schlüssel
106
Netzwerk
108
110
108
110
112
Stochastische Daten
114
Stochastischer Prozeß
116
Datenquelle

FIG 1

FIG 2

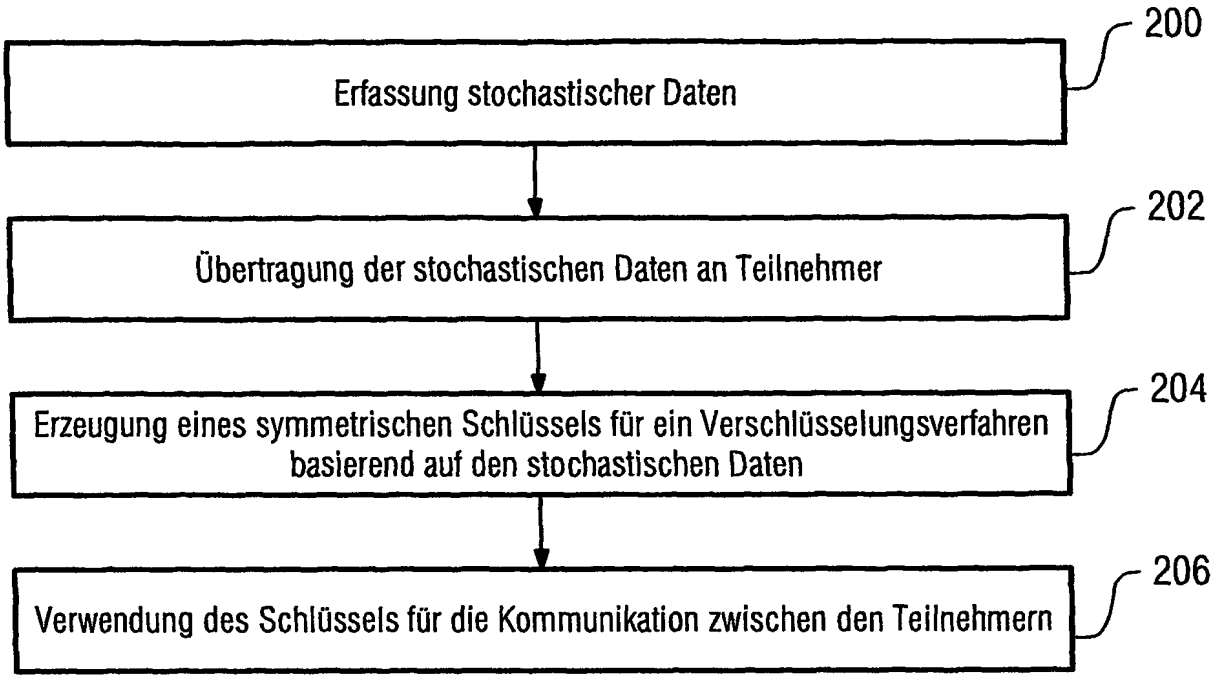
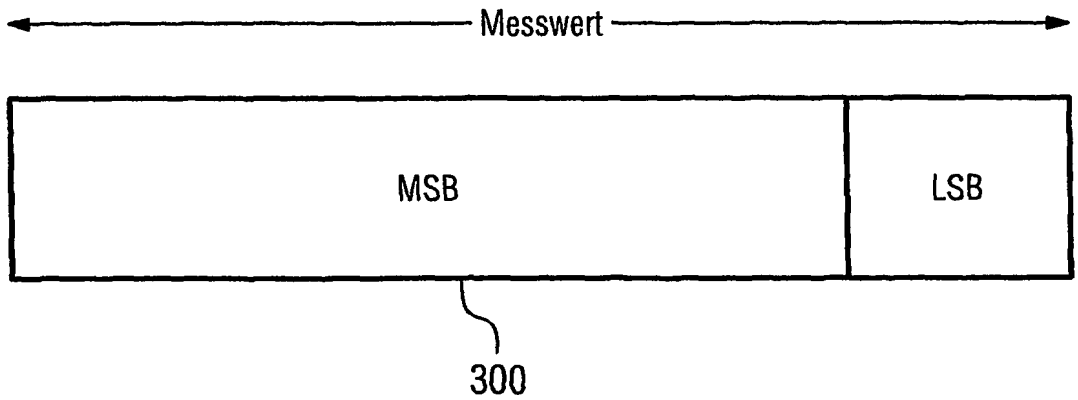

200
Erfassung stochastischer Daten
202
Übertragung der stochastischen Daten an Teilnehmer
204
Erzeugung eines symmetrischen Schlüssels für ein Verschlüsselungsverfahren basierend auf den stochastischen Daten
206
Verwendung des Schlüssels für die Kommunikation zwischen den Teilnehmern

FIG 3


Messwert
MSB
LSB
300

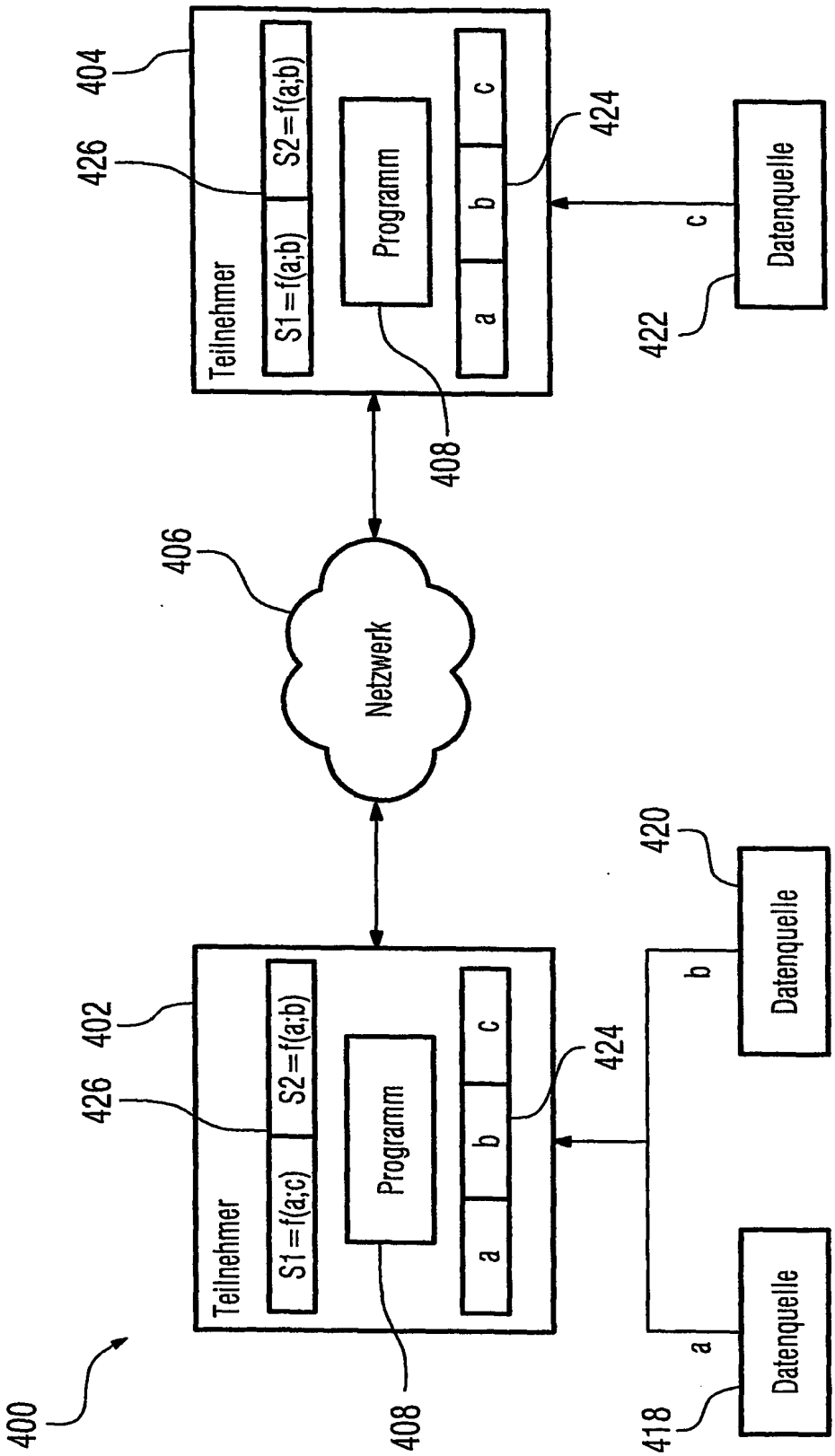
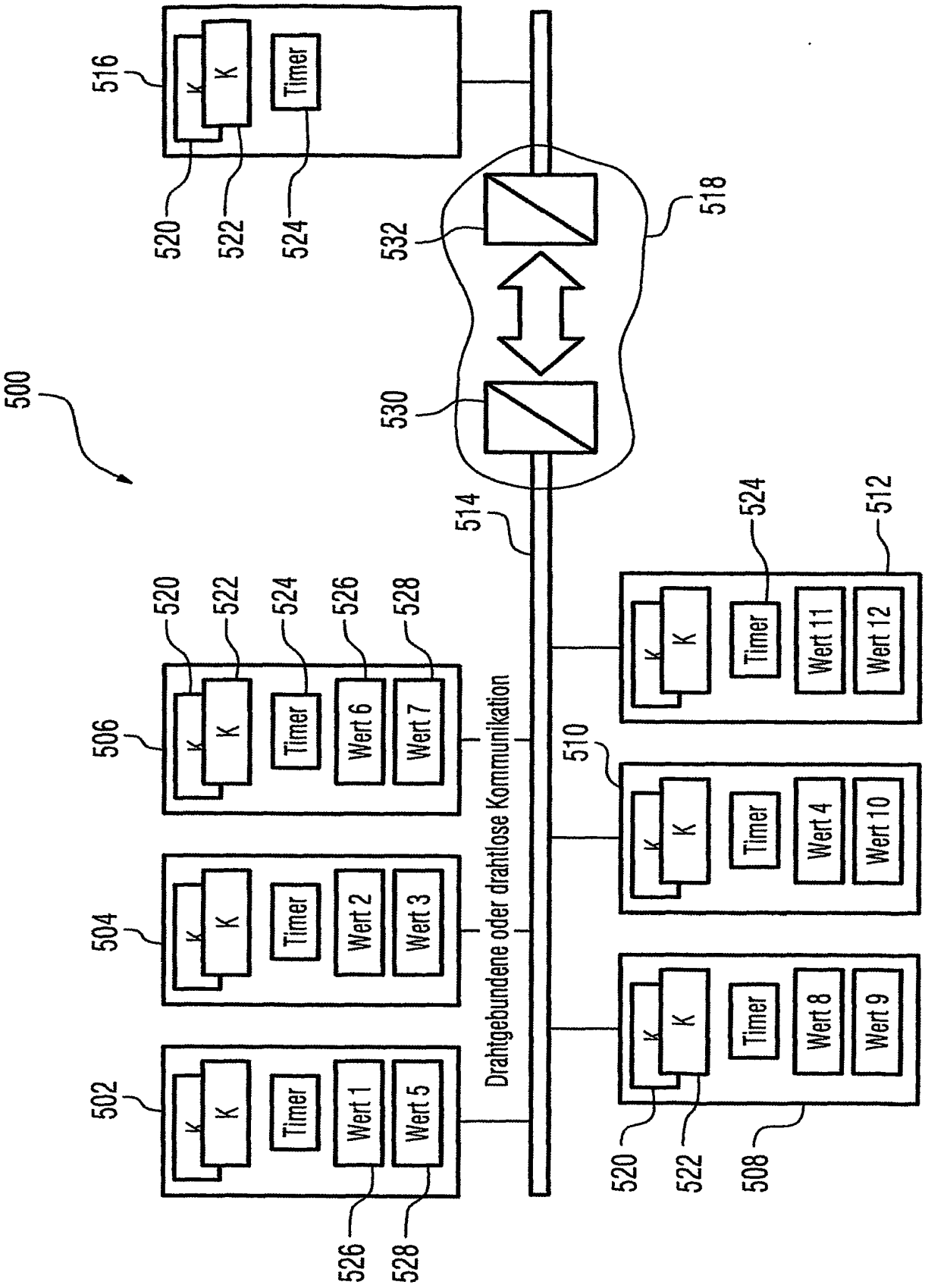

400
402
404
406
408
418
420
422
424
426
Teilnehmer
S1=f(a;b)
S2=f(a;b)
S1=f(a;c)
Programm
a
b
c
Netzwerk
Datenquelle

FIG 4


500
502
504
506
508
510
512
514
516
518
520
522
524
526
528
530
532
K
Timer
Wert 1
Wert 2
Wert 3
Wert 4
Wert 5
Wert 6
Wert 7
Wert 8
Wert 9
Wert 10
Wert 11
Wert 12
Drahtgebundene oder drahtlose Kommunikation

INTERNATIONAL SEARCH REPORT

Int[illegible]nal Application No
PCT/EP2004/007378

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08 G06F7/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97/49213 A (ERICSSON GE MOBILE INC) 24 December 1997 (1997-12-24) page 1, line 5 - page 2, line 5 page 4, line 5 - page 5, line 14	1-24
X	US 2002/034300 A1 (HANSEN MADS DORE ET AL) 21 March 2002 (2002-03-21) paragraph '0001! - paragraph '0013! paragraph '0074! - paragraph '0077! paragraph '0080! paragraph '0102! - paragraph '0103!	1-24
A	WO 02/063462 A (CAMBRIDGE SILICON RADIO LTD ; COLLIER JAMES DIGBY YARLET (GB)) 15 August 2002 (2002-08-15) page 1, line 1 - page 2, line 16 page 3, line 8 - page 8, line 4	1-24

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 October 2004	03/11/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Liebhardt, I

1

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/007378

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9749213 A	24-12-1997	US 5745578 A	28-04-1998
		AU 723304 B2	24-08-2000
		AU 3151197 A	07-01-1998
		CA 2257645 A1	24-12-1997
		CN 1222275 A ,B	07-07-1999
		EP 0906679 A1	07-04-1999
		ID 17049 A	04-12-1997
		JP 2000512825 T	26-09-2000
		KR 2000016713 A	25-03-2000
		US 6031913 A	29-02-2000
		WO 9749213 A1	24-12-1997
US 2002034300 A1	21-03-2002	SE 516567 C2	29-01-2002
		AU 6448001 A	17-12-2001
		AU 6450101 A	17-12-2001
		EP 1293061 A1	19-03-2003
		EP 1292882 A1	19-03-2003
		JP 2003536299 T	02-12-2003
		SE 0002158 A	08-12-2001
		WO 0195559 A1	13-12-2001
		WO 0195091 A1	13-12-2001
		US 2002035687 A1	21-03-2002
WO 02063462 A	15-08-2002	CN 1488094 T	07-04-2004
		EP 1364279 A2	26-11-2003
		WO 02063462 A2	15-08-2002
		JP 2004519035 T	24-06-2004
		US 2002107897 A1	08-08-2002

INTERNATIONALER RECHERCHENBERICHT

In onales Aktenzeichen
PCT/EP2004/007378

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/08 G06F7/58

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 97/49213 A (ERICSSON GE MOBILE INC) 24. Dezember 1997 (1997-12-24) Seite 1, Zeile 5 - Seite 2, Zeile 5 Seite 4, Zeile 5 - Seite 5, Zeile 14	1-24
X	US 2002/034300 A1 (HANSEN MADS DORE ET AL) 21. März 2002 (2002-03-21) Absatz '0001! - Absatz '0013! Absatz '0074! - Absatz '0077! Absatz '0080! Absatz '0102! - Absatz '0103!	1-24
A	WO 02/063462 A (CAMBRIDGE SILICON RADIO LTD ; COLLIER JAMES DIGBY YARLET (GB)) 15. August 2002 (2002-08-15) Seite 1, Zeile 1 - Seite 2, Zeile 16 Seite 3, Zeile 8 - Seite 8, Zeile 4	1-24

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
26. Oktober 2004	03/11/2004

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Liebhardt, I

1

INTERNATIONALER RECHERCHENBERICHT

Internales Aktenzeichen
PCT/EP2004/007378

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9749213 A	24-12-1997	US 5745578 A	28-04-1998
		AU 723304 B2	24-08-2000
		AU 3151197 A	07-01-1998
		CA 2257645 A1	24-12-1997
		CN 1222275 A ,B	07-07-1999
		EP 0906679 A1	07-04-1999
		ID 17049 A	04-12-1997
		JP 2000512825 T	26-09-2000
		KR 2000016713 A	25-03-2000
		US 6031913 A	29-02-2000
		WO 9749213 A1	24-12-1997
US 2002034300 A1	21-03-2002	SE 516567 C2	29-01-2002
		AU 6448001 A	17-12-2001
		AU 6450101 A	17-12-2001
		EP 1293061 A1	19-03-2003
		EP 1292882 A1	19-03-2003
		JP 2003536299 T	02-12-2003
		SE 0002158 A	08-12-2001
		WO 0195559 A1	13-12-2001
		WO 0195091 A1	13-12-2001
		US 2002035687 A1	21-03-2002
WO 02063462 A	15-08-2002	CN 1488094 T	07-04-2004
		EP 1364279 A2	26-11-2003
		WO 02063462 A2	15-08-2002
		JP 2004519035 T	24-06-2004
		US 2002107897 A1	08-08-2002